

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001273498 A**

(43) Date of publication of application: 05.10.01

(51) Int. Cl.

G06T 7/00

A61B 5/117

G06F 15/00

G06K 17/00

G06K 19/10

G06T 1/00

H04L 9/32

(21) Application number: **2000085133**

(22) Date of filing: 24.03.00

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

(72) Inventor: **TAMAI SEIICHIRO**

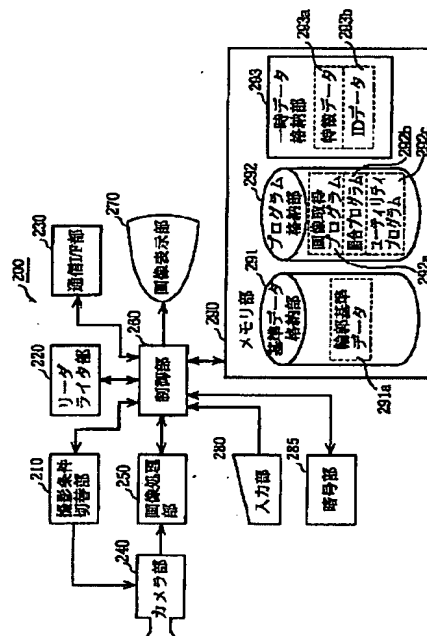
(54) **DEVICE, SYSTEM, CARD AND METHOD FOR PERSONAL IDENTIFICATION BASED ON BIOMETRIC**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an authentication device for accurately performing personal authentication without giving a psychologically unpleasant feeling or a hateful feeling to a user.

SOLUTION: This device is provided with a camera part 240 and an image processing part 250 for acquiring a biometric image by photographing a part (fingerprint or iris or the like) of a body without contact, an image display part 270 for overlapping and displaying a guiding image for guiding that part to an optimal photographing position and the biometric image, a control part 260 and a communication I/F part 230 or the like for extracting feature data from the acquired biometric image, enciphering these data by means of a cipher part 285 and transmitting them to an authentication server 30 later.

COPYRIGHT: (C)2001,JPO



【特許請求の範囲】

【請求項 1】 バイオメトリックに基づいて本人認証を行う装置であって、非接触で身体の一部を撮影することによりバイオメトリック画像を取得する撮影手段と、取得されたバイオメトリック画像を表示するバイオメトリック画像表示手段と、

適正な撮影位置で前記部位が撮影された場合の部位の外形を示すガイド画像を前記バイオメトリック画像に重ねて表示するガイド表示手段と、

前記バイオメトリック画像に基づいて、前記部位が適正な撮影位置で撮影されたか否かを判断する判断手段と、適正な撮影位置で撮影されたか判断された場合に、前記バイオメトリック画像から前記部位の形態的な特徴を示すバイオメトリック情報を抽出し、予め登録されたバイオメトリック情報と照合することにより、本人認証を行う認証手段とを備えることを特徴とする本人認証装置。

【請求項 2】 前記本人認証装置は、さらに、適正な撮影位置で前記部位が撮影されるように前記撮影手段による撮影の方向と倍率とを制御する撮影制御手段を備えることを特徴とする請求項 1 記載の本人認証装置。

【請求項 3】 前記本人認証装置は、さらに、前記部位又は前記部位を含むより大きな部位を繰り返して撮影するように前記撮影手段を制御し、得られた複数の画像に基づいて、身体の一部を検出する動き検出手段を備え、前記認証手段は、前記動き検出手段によって身体の一部が検出され、かつ、前記部位が適正な撮影位置で撮影されたか判断された場合に、本人認証を行うことを特徴とする請求項 1 記載の本人認証装置。

【請求項 4】 前記部位は、虹彩であり、前記動き検出手段は、前記虹彩に光を照射するとともに、その照射に同期して虹彩を撮影するように前記撮影手段を制御することを特徴とする請求項 3 記載の本人認証装置。

【請求項 5】 前記本人認証装置は、さらに、繰り返して前記部位を撮影するように前記撮影手段を制御する繰り返し制御手段を備え、前記認証手段は、繰り返し撮影によって得られた複数のバイオメトリック画像に基づいて前記バイオメトリック情報を抽出し、本人認証を行うことを特徴とする請求項 1 記載の本人認証装置。

【請求項 6】 前記本人認証装置は、さらに、身体の一部の部位について、前記バイオメトリック画像を取得し、取得されたバイオメトリック画像を表示し、前記ガイド画像を表示し、前記部位が適正な撮影位置で撮影されたか否かを判断するように前記撮影手段と、前記バイオメトリック画像表示手段と、前記ガイド表示手段と、判断手段とを制御する複数部位制御手段を備え、前記認証手段は、取得された複数の部位のバイオメトリック画像から複数の部位についてのバイオメトリック情

報を抽出し、それらバイオメトリック情報の組み合わせと予め登録された対応するバイオメトリック情報の組み合わせとを照合することにより、本人認証を行うことを特徴とする請求項 1 記載の本人認証装置。

【請求項 7】 前記認証手段は、前記複数の部位ごとの照合結果を示す一致度それぞれに異なる重みづけをした後に加算して得られる総合評価値が一定のしきい値を超えるか否かによって、前記本人認証を行うことを特徴とする請求項 6 記載の本人認証装置。

10 【請求項 8】 前記複数の部位は、指紋と虹彩であることを特徴とする請求項 6 記載の本人認証装置。

【請求項 9】 前記複数の部位は、異なる指の指紋であることを特徴とする請求項 6 記載の本人認証装置。

【請求項 10】 前記複数の部位は、両目の虹彩であることを特徴とする請求項 6 記載の本人認証装置。

【請求項 11】 前記本人認証装置は、さらに、前記撮影に伴って、本人の識別に役立つ情報である ID データを取得する ID データ取得手段を備え、

20 前記認証装置は、前記バイオメトリック情報及び前記 ID データの組み合わせと予め登録されたバイオメトリック情報及び ID データの組み合わせとを照合することにより、本人認証を行うことを特徴とする請求項 1 記載の本人認証装置。

【請求項 12】 前記認証手段は、予め登録された複数のバイオメトリック情報の中から、ID データが一致するものを特定し、特定したバイオメトリック情報と抽出された前記バイオメトリック情報との同一性によって、本人認証を行うことを特徴とする請求項 1 記載の本人認証装置。

30 【請求項 13】 前記認証装置は、さらに、予め登録された前記バイオメトリック情報を記憶する記憶手段と、

前記記憶手段に記憶されたバイオメトリック情報を前記認証手段により抽出されたバイオメトリック情報で置き換える登録情報更新手段を備えることを特徴とする請求項 1 記載の本人認証装置。

【請求項 14】 前記更新手段は、予め定められた一定期間を超えてバイオメトリック情報が更新されていない場合に、前記バイオメトリック情報を置き換えることを特徴とする請求項 1 3 記載の本人認証装置。

【請求項 15】 通信ネットワークを介して接続された認証端末と認証サーバとからなるバイオメトリックに基づく本人認証システムであって、

前記認証端末は、非接触で身体の一部を撮影することによりバイオメトリック画像を取得する撮影手段と、

取得されたバイオメトリック画像を表示するバイオメトリック画像表示手段と、

50 適正な撮影位置で前記部位が撮影された場合の部位の外形を示すガイド画像を前記バイオメトリック画像に重ね

て表示するガイド表示手段と、
前記バイオメトリック画像に基づいて、前記部位が適正な撮影位置で撮影されたか否かを判断する判断手段と、適正な撮影位置で撮影されたと判断された場合に、前記バイオメトリック画像から前記部位の形態的な特徴を示すバイオメトリック情報を抽出し、前記認証サーバに送信するバイオメトリック情報抽出手段とを備え、

前記認証サーバは、

予め登録された複数のバイオメトリック情報を記憶するバイオメトリック情報記憶手段と、

前記認証端末から送信されてきたバイオメトリック情報と前記バイオメトリック情報記憶手段に記憶されたバイオメトリック情報とを照合することにより、本人認証を行う認証手段とを備えることを特徴とする本人認証システム。

【請求項16】 前記認証端末は、さらに、前記撮影に伴って、本人の識別に役立つ情報であるIDデータを取得するIDデータ取得手段と、

取得されたIDデータを認証サーバに送信することにより、そのIDデータと一致するIDデータに対応するバイオメトリック情報を前記認証サーバからダウンロードするダウンロード手段と、

ダウンロードされたバイオメトリック情報と前記バイオメトリック情報抽出手段により抽出されたバイオメトリック情報とを照合することにより、本人認証を行う認証手段とを備え、

前記認証サーバは、さらに、

前記バイオメトリック情報記憶手段に記憶された複数のバイオメトリック情報それぞれに対応するIDデータを予め記憶するIDデータ記憶手段と、

前記バイオメトリック情報記憶手段及び前記IDデータ記憶手段を参照することにより、前記認証端末から送信されたきたIDデータと一致するIDデータに対応するバイオメトリック情報を読み出して前記認証端末に送信するバイオメトリック情報送信手段とを備えることを特徴とする請求項15記載の本人認証システム。

【請求項17】 バイオメトリックに基づく本人認証に用いられる携帯型のカードであって、身体の一部の形態的な特徴を示すバイオメトリック情報を記憶するバイオメトリック情報記憶手段と、身体の一部を示す画像データを外部から取得する画像データ取得手段と、

取得された画像データからバイオメトリック情報を抽出し、前記バイオメトリック情報記憶手段に記憶されたバイオメトリック情報と照合することにより、本人認証を行う認証手段とを備えることを特徴とする本人認証用カード。

【請求項18】 請求項1記載の本人認証装置が組み込まれた携帯電話機。

【請求項19】 請求項1記載の本人認証装置が組み込

まれたパーソナルコンピュータ。

【請求項20】 ビルディングへの人の出入りを管理するビル管理システムであって、

請求項1記載の本人認証装置と、

前記認証装置により本人認証が成功した場合に、前記ビルディングに出入りするための扉を開錠する制御手段とを備えることを特徴とするビル管理システム。

【請求項21】 請求項1記載の本人認証装置と、

前記認証装置により本人認証が成功した場合に、エンジン始動を許可する制御手段とを備えることを特徴とする自動車。

【請求項22】 請求項1記載の本人認証装置と、

前記認証装置により本人認証が成功した場合に、指定された商品を取り出し口に移動させる制御手段とを備えることを特徴とする自動販売機。

【請求項23】 請求項1記載の本人認証装置と、

前記認証装置による本人認証の結果に応じて入出金処理を行う入出金処理手段とを備えることを特徴とする現金自動預払機。

【請求項24】 請求項1記載の本人認証装置と、

前記認証装置による本人認証の結果に応じて入出金処理を行う入出金処理手段とを備えるPOS端末装置。

【請求項25】 通信ネットワークを介して接続された認証端末と認証サーバとから構成され、バイオメトリックに基づく本人認証による電子決済を行うためのシステムであって、

前記認証端末は、

操作者から電子決済を行いたい旨の要求を受け付ける受付手段と、

30 非接触で前記操作者の身体の一部を撮影することによりバイオメトリック画像を取得する撮影手段と、

取得されたバイオメトリック画像を表示するバイオメトリック画像表示手段と、

適正な撮影位置で前記部位が撮影された場合の部位の外形を示すガイド画像を前記バイオメトリック画像に重ねて表示するガイド表示手段と、

前記バイオメトリック画像に基づいて、前記部位が適正な撮影位置で撮影されたか否かを判断する判断手段と、

適正な撮影位置で撮影されたと判断された場合に、前記バイオメトリック画像から前記部位の形態的な特徴を示すバイオメトリック情報を抽出し、前記電子決済を特定する情報とともに前記認証サーバに送信するバイオメトリック情報抽出手段とを備え、

40 前記認証サーバは、

予め登録された複数のバイオメトリック情報を記憶するバイオメトリック情報記憶手段と、

前記認証端末から送信されてきたバイオメトリック情報と前記バイオメトリック情報記憶手段に記憶されたバイオメトリック情報とを照合することにより、本人認証を

行う認証手段と、

50 行う認証手段と、

本人認証に成功したときに、前記認証端末から送られてきた情報によって特定される電子決済を行う決済手段とを備えることを特徴とする電子決済システム。

【請求項26】 バイオメトリックに基づいて本人認証を行う方法であって、非接触で身体の一部を撮影する撮影手段を制御することによりバイオメトリック画像を取得する撮影ステップと、

取得されたバイオメトリック画像を表示手段に表示するバイオメトリック画像表示ステップと、

適正な撮影位置で前記部位が撮影された場合の部位の外形を示すガイド画像を前記バイオメトリック画像に重ねて前記表示手段に表示するガイド表示ステップと、

前記バイオメトリック画像に基づいて、前記部位が適正な撮影位置で撮影されたか否かを判断する判断ステップと、

適正な撮影位置で撮影されたと判断された場合に、前記バイオメトリック画像から前記部位の形態的な特徴を示すバイオメトリック情報を抽出し、予め登録されたバイオメトリック情報と照合することにより、本人認証を行う認証ステップとを含むことを特徴とする本人認証方法。

【請求項27】 バイオメトリックに基づいて本人認証を行うためのプログラムが記録されたコンピュータ読み取り可能な記録媒体であって、

前記プログラムは、請求項26記載のステップをコンピュータに実行させることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、バイオメトリックに基づいて本人認証を行う装置、その装置を利用して金融・流通等の決済を行うシステム、そのための携帯型カード及び本人認証方法等に関する。

【0002】

【従来の技術】 電子商取引やカード決済等においては、パスワードや署名等によって本人認証が行われる。ところが、これらパスワードや署名は、盗聴や偽造、なりすまし等の不正行為による攻撃を受け易い。そのために、最近では、より高いセキュリティを維持するために、バイオメトリック（生体測定）に基づく本人認証が行われている。その代表的なものに、バイオメトリックセンサによって指紋の画像を取得し、予め登録しておいた指紋画像と照合することによって生体を識別し、本人認証を行う認証装置がある（特開2000-30028号公報の「認証装置」等）。

【0003】 図18は、従来の認証装置が備えるバイオメトリックセンサの例を示す。図18(a)は、光学式指紋スキャナと呼ばれる方式であり、プリズム等のガラス面に押圧された指の指紋をCCD等を用いてスキャンすることで、光学的に指紋画像を読み取る方式である。

図18(b)は、静電容量型指紋センサチップによる方式であり、コンデンサアレイが形成された半導体センサの表面に指が置かれたときの各コンデンサの静電容量を検出することにより指紋画像を読み取る方式である。

【0004】 このようにして読み取った指紋画像と予め登録しておいた指紋画像とを照合することにより本人認証が行われている。

【0005】

【発明が解決しようとする課題】 ところが、上記のようなバイオメトリックセンサによる従来の認証装置は、以下の問題を有している。

(1) ガラス面に指を接触させて指紋の画像を取得する方式に起因する以下の問題がある。

【0006】 つまり、繰り返し使用によってガラス面が汚れるので、定期的にガラス面をクリーニングする等の保守が必要とされる。また、静電気が生じ易いこと、及び、指の押圧がかかること等を考慮すると、上述の半導体センサは十分に実用に耐え得るとは言えない。さらに、他人が触れたガラス面に触りたくないという嫌悪感をいなくユーザを考慮する必要もある。

(2) 指紋の読取専用のバイオメトリックセンサを備える必要があるために、装置全体がコスト高となってしまう。

(3) 指紋だけを用いて本人認証をしていることに基づく以下の問題がある。

【0007】 つまり、指に包帯を巻いていたり、火傷や擦り切れたために指紋を採取することが困難なユーザに対しては、もはや本人認証を実施することができない。また、指紋画像を用いた認証の精度が必ずしも十分に高いとは言えない。そこで、本発明は、かかる問題点を鑑みてなされたものであり、バイオメトリックセンサの保守がほとんど不要であり、静電気や押圧に対する問題を生じることがなく、かつ、ユーザに心理的な不快感や嫌悪感を与えることなくバイオメトリック画像を取得して本人認証を行う認証装置等を提供することを第1の目的とする。

【0008】 また、低コストで、かつ、精度の高い本人認証を行う認証装置等を提供することを第2の目的とする。

【0009】

【課題を解決するための手段】 上記第1の目的を達成するために、本発明に係る認証装置等は、ビデオカメラを用いて、非接触でバイオメトリック画像を取り込むことを特徴とする。そのために、認証装置は、表示画面を有し、その表示画面に、カメラが撮影している画像と適正な撮影位置を示すガイド画像とを表示する。ユーザは、認証装置の表示画面に映し出された自分の指とガイド画像とが重なるように、指の位置を移動させればよい。これによって、非接触センシングによる鮮明なバイオメトリック画像の取り込みが実現され、接触センシングに起

因する従来の問題が解消される。

【0010】また、上記第2の目的を達成するために、本発明に係る認証装置が備えるカメラは、指紋だけでなく、虹彩（アイリス）、掌形、顔形等の複数のバイOMETリック画像を取り込み、それら画像による複数の識別結果を組み合わせて本人認証を行う。これによって、認証精度が向上されるとともに、異なる種別のバイOMETリック画像それぞれを取得するための複数のセンサを備える場合に比べ、極めて低コストによる本人認証が実現される。

【0011】また、取得したバイOMETリック画像と照合する基準データ（予め登録されたバイOMETリック情報）については、一定期間ごと、又は、ユーザからバイOMETリック画像を取得する度に、最新の内容に更新していく。これによって、基準データが最新のものに維持され、高い精度による本人認証が維持される。また、取得したバイOMETリック画像と基準データとの照合において、バイOMETリック画像だけでなく、ユーザから取得した名前や生年月日等のIDデータを組み合わせて照合する。例えば、照合の対象となる個人データの候補をIDデータによって絞り込んでおいた後に、バイOMETリック画像に基づく照合を行う。これによって、本人認証の精度が向上されるとともに、本人認証に要する時間が短縮される。

【0012】

【発明の実施の形態】以下、本発明の実施の形態について、図面を用いて説明する。図1は、本発明に係る電子マネーシステム10の全体構成を示す図である。この電子マネーシステム10は、バイOMETリックに基づく本人認証によって消費者が電子決済を行うことが可能なシステムであり、インターネット等の通信ネットワーク20を介して接続された認証サーバ30、ゲートウェイ40、携帯電話機50、PDA（Personal Digital Assistance；携帯情報端末）60、ATM（Automated Teller Machine；現金自動預払機）70、PC（Personal Computer）80、銀行用通信端末90及び電子ショップ用通信端末100等から構成される。

【0013】この電子マネーシステム10においては、消費者のバイOMETリック画像（ここでは、少なくとも指紋及び虹彩のいずれかの画像）は、各通信装置50、60、70及び80が備えるカメラによって非接触に取得され、本人認証のための必須の情報となっている。一方、IDカード110は、バイOMETリック画像に基づく本人認証を補助するために用いられる。

【0014】認証サーバ30は、携帯電話機50、PDA60及びPC80から送られてくる特徴データ（バイOMETリック画像から抽出された指紋又は虹彩の特徴を示すデータ）を受信し、予めデータベースとして登録された特徴データと照合することによって本人認証を行い、その結果を取引先の電子ショップや銀行に報告する

等の決済処理等を集中的に実行するコンピュータである。

【0015】ここで、認証サーバ30に備えられているデータベースは、図2に示されるように、この電子マネーシステム10を利用する全ての会員（消費者）について、PIC（Personal Identification Code；個人識別コード）、IDデータ（IDカード110に記録されている個人識別情報）、その会員のバイOMETリック画像、そのバイOMETリック画像から抽出された特徴データ、それらバイOMETリック画像及び特徴データが登録された年月日等を対応づけて集めたものである。なお、この電子マネーシステム10では、本人認証の精度を確保するために、バイOMETリック画像と特徴データのうち、少なくとも2つの特徴データが登録されていることが条件とされる。

【0016】この認証サーバ30は、ATM70等から、特徴データを参照したい旨の要求をIDデータと共に受け取った場合には、そのIDデータが一致する特徴データをデータベース中で検索し、該当する全ての特徴データを読み出して暗号化した後にATM70等の要求元に返信するというデータ配信機能も有する。さらに、この認証サーバ30は、本人認証に成功し、かつ、その本人についての特徴データが一定期間（例えば、3年）を超えて更新されていない場合は、携帯電話機50等から送られてきた最新の特徴データで古い特徴データを置き換えることにより、データベースを更新したり、この電子マネーシステム10の新規会員に対してIDカード110を発行する機能も有する。

【0017】銀行用通信端末90は、銀行に設置されたコンピュータであり、消費者、認証サーバ30及びATM70等からの通信による決済の指示に従って、入出金や振替等の金融処理を行う。電子ショップ用通信端末100は、ネットワーク上で商品を販売する販売主が所有するコンピュータであり、消費者、認証サーバ30等からの注文指示等を受けて販売処理を行う。

【0018】ゲートウェイ40は、携帯電話機50やPDA60等による無線電話網と通信ネットワーク20とを接続する無線基地局等である。携帯電話機50及びPDA60は、それぞれ、一般的な携帯電話機及び携帯情報端末としての機能に加えて、内蔵する小型カメラにより、操作者のバイOMETリック画像を取得し、その画像から特徴データを生成して認証サーバ30に送信することによって、その場での電子決済を可能とする移動端末としての機能を有する。操作者は、カードを用いたり、パスワードを入力したりすることなく、携帯電話機50及びPDA60の表示画面と対話するだけで、希望商品を注文する等の商取引を行うことができる。

【0019】ATM70は、一般的な現金自動預払機の機能に加えて、ビデオカメラにより、操作者のバイOMETリック画像を取得し、その画像又はその画像とIDカ

10

20

30

40

50

ード110から読み出したIDデータとに基づいて、認証サーバ30と通信しながら、又は、認証サーバ30と通信することなく（スタンドアローンで）、本人認証を遂行し、その結果に応じて入出金処理を行う機能を有する。

【0020】つまり、操作者は、IDカード110を所持している場合にはATM70にそのIDカード110を挿入した後に本人認証を終えることで、また、IDカード110を所持していない場合であっても本人認証を終えることで、パスワード等を入力することなく、自分の口座からお金を引き出ししたりすることができる。PC80は、オフィスや家庭に設置されるコンピュータであり、一般的なコンピュータとしての機能に加えて、上記PDA60が有する機能や、自分のIDカード110に記録されている特徴データを更新する等の機能を有する。操作者は、このPC80の表示画面と対話すること、希望商品を注文したり、IDカード110の内容を書き換えることによる保守をしたりすることができる。

【0021】図3(a)～(c)は、この電子マネージシステム10で用いられるIDカード110の種別を示す図である。ここには、3種類のIDカード110a～cが示されている。図3(a)に示されたIDカード110bは、最も簡易なタイプ1のIDカードであり、表面に磁気ストライプや光学メモリが形成されたプラスチックカードである。これら磁気ストライプや光学メモリには、持主のIDデータ（名前、生年月日、住所、電話番号、パスワード）が記録されている。これらIDデータは、例えば、ATM70により本人認証が行われる際に、照合対象となる特徴データを認証サーバ30中で検索するときの検索キーとして用いられる。

【0022】図3(b)に示されたIDカード110bは、上記IDカード110aによる磁気メモリ又は光学メモリに加えて、表面に電極を露出させた不揮発性ICメモリ（フラッシュメモリ）を内蔵している。このICメモリには、持主の特徴データが記録される。この特徴データは、例えば、ATM70によるその場での本人認証、即ち、そのIDカード110bの使用者と持主との同一性を判断する等のための用いられる。具体的には、ATM70のカメラを介して取得された使用者の特徴データとATM70に挿入されたIDカード110bに記録されていた特徴データとの同一性が判断される。

【0023】図3(c)に示されたIDカード110cは、最も高機能なIDカードであり、上記IDカード110bに備えられている磁気又は光学メモリ及びICメモリに加えて、本人認証を自ら実行するための認証回路を内蔵している。このIDカード110cは、認証処理を実行するためのプログラムを格納したROM及びそのプログラムを実行するCPU等からなる回路を備え、ATM70やPC80のカメラを介して取得された特徴データと内部のICメモリに記録されている特徴データと

の同一性を自ら判断する。従って、このIDカード110cが用いられた場合には、認証サーバ30やATM70での認証処理は不要となる。

【0024】図4は、図1に示されたATM70が備える認証装置200、即ち、ATM70のうち本発明に係る本人認証に関連する部分の構成を示すブロック図である。なお、携帯電話機50、PDA60、PC80及び認証サーバ30についても、この認証装置200と同一の構成又はそのサブセット（一部の構成）が内蔵されている。

【0025】この認証装置200は、操作者と対話しながら非接触でバイOMETリック画像を取得し、その画像から特徴データを抽出した後に、認証サーバ30やIDカード110に登録された特徴データと照合することにより、本人認証を実行する（又は、認証サーバ30やIDカード110cに実行させる）装置であり、撮影条件切替部210、リーダライタ部220、通信I/F（Interface）部230、カメラ部240、画像処理部250、制御部260、画像表示部270、入力部280、暗号部285及びメモリ部290から構成される。

【0026】カメラ部240は、本人認証に用いられる身体の一部（ここでは、指紋及び虹彩）を撮影し、カラーの画像信号を出力する小型ビデオカメラ等である。図5は、カメラ部240の詳細な構成を示すブロック図である。このカメラ部240は、Z駆動部243、撮像レンズ244、イメージセンサ部245及びAF制御部246からなる可動のアセンブリである可動部241と、θ駆動部242と、キャプチャ制御部247と、発光部248とから構成される。

【0027】撮像レンズ244は、広角のズームレンズである。Z駆動部243は、撮像レンズ244をZ方向（遠近方向）に駆動するアクチュエータ等であり、撮影条件切替部210からの指示に基づいて撮像レンズ244をズームングすることにより、撮影倍率を変化させたり、AF制御部246からの指示に基づいて撮像レンズ244をZ方向に微小移動させることにより、フォーカシングを行う。

【0028】AF制御部246は、発光部248等から発せられた光の反射光をイメージセンサ部245等で検出させることによって、被写体までの距離を計測し、その距離に応じてZ駆動部243を制御する自動焦点調整回路である。イメージセンサ部245は、例えば、350×400画素のCMOSイメージセンサ等からなる撮像素子である。なお、CMOSイメージセンサは、CPU等の回路と一体化させることが容易であり、低消費電力である点で、このイメージセンサ部245の材料として好ましい。

【0029】θ駆動部242は、撮影条件切替部210からの指示に基づいて、ジャイロ機構等により可動部241を2次元的に回転（地面に水平及び垂直方向に回

10

20

30

40

50

転) させるアクチュエータ等である。発光部248は、自動焦点調整及びストロボ用の光を発光するLEDやフラッシュ回路等である。

【0030】キャプチャ制御部247は、撮影条件切替部210からの指示に基づいて、イメージセンサ部245に対して画像をサンプリングする(カラーイメージを保持する)旨の指示を出したり、発光部248に対してストロボ発光等を指示したりする。発光部248にストロボ発光を指示したときには、このキャプチャ制御部247は、ストロボ発光と同期させて(被写体の瞳孔が小さくなった瞬間に)画像をサンプリングするようイメージセンサ部245に指示を出す。

【0031】撮影条件切替部210は、制御部260から、撮像条件(段階的に設定された複数の撮影倍率の1つ及び複数の撮影方向の1つ)や微調整のための指示を受け取り、その条件や指示に対応する制御信号をカメラ部240のZ駆動部243及びθ駆動部242に送ることによって、カメラ部240の撮影倍率と撮影方向を粗く変化させたり、微調整したりする。これによって、カメラ部240による被写体(操作者の身体部位)の追尾制御が行われ、イメージセンサ部245上の予め定められた最適位置に最適なサイズでバイOMETリック画像が結像される。

【0032】また、撮影条件切替部210は、制御部260から虹彩を撮影する旨の指示を受けた場合には、キャプチャ制御部247に対して、上述のようなストロボ発光と同期した撮影(以下、「ストロボ同期撮影」という。)を行うように指示する。これは、照度が十分でない場所においても、瞳孔を絞り込んだ状態での虹彩、即ち、大きな面積を有する虹彩の撮影と可能としたり、生体が生きていることの確認をしたりするためである。

【0033】なお、携帯電話機50及びPDA60に装備される認証装置は、ATM70に装備される認証装置200とは異なり、カメラ部240のZ駆動部243及び撮影条件切替部210を備えておらず、固定化された撮影倍率と撮影方向で被写体を撮影する(ただし、AF制御部246による自動焦点調整及びキャプチャ制御部247によるストロボ同期撮影は行われる)。

【0034】つまり、携帯電話機50及びPDA60に装備される認証装置は、予め定められた適正な空間位置に被写体が置かれることを前提としている。ただし、そのような適正位置に被写体を誘導するために、画像表示部270にガイド画像(被写体の適正な撮影位置を示す画像)を表示する。画像処理部250は、AD変換器、バッファメモリ、デジタルフィルタ(スムージング、エッジ検出、特徴抽出用フィルタ)及び演算器等からなり、制御部260からの指示に従って、カメラ部240のイメージセンサ部245から送られてきたカラー画像の信号をデジタル化し、得られたバイOMETリック画像のデータに対して必要なフィルタリング処理等を行うと

とで被写体の輪郭や特徴を抽出する。

【0035】つまり、画像処理部250は、制御部260からの要求に従って、(i)カメラ部240により撮影されたカラー画像の全て(バイOMETリック画像の全体)、(ii)指又は目の輪郭位置を示す輪郭データ、(iii)その輪郭に囲まれた部分の画像(切り出されたバイOMETリック画像)、及び、(iv)指紋の特徴点等を特定するデータ(指紋の特徴データ)又は虹彩の特徴を示すアイリスコード(虹彩の特徴データ)のいずれかを生成し、制御部260に渡す。

【0036】図6は、画像処理部250が生成する指紋の特徴データを説明するための図である。特徴データは、指紋の特徴点(分岐点及び端点)や中心点の相対位置、隆線の位置及び方向が数値化されたものである。図7は、画像処理部250が生成する虹彩の特徴データを説明するための図である。虹彩とは、黒目の内側で瞳孔より外側のドーナツ状の部分でいい、瞳孔の開き具合を調節する筋肉から構成される。虹彩の特徴データは、虹彩の中心を原点とする極座標において半径方向と回転方向とに予め分割された複数の領域それぞれにおけるアイリスパターン(放射状に描かれる虹彩のパターン)の濃淡を示す2値データが符号化されたもの(256バイトのアイリスコード等)である。

【0037】リーダーライタ部220は、3種類のIDカード110a～cに対応した記録再生装置であり、装着されたIDカード110に記録されたIDデータ及び特徴データを読み出したり、IDカード110に特徴データを書き込んだりする。通信I/F部230は、モデムカード、LANカード及び無線による送受信回路等であり、ゲートウェイ40や通信ネットワーク20等を介してこの認証装置200が認証サーバ30等と通信するためのインタフェース回路である。

【0038】画像表示部270は、携帯電話機50等が備えるカラーLCDやATM70等が備えるカラーCRT等であり、本認証装置200においては、本人認証の際に操作者の指や目を適正な撮影位置に誘導する際のガイド表示等のために用いられる。入力部280は、携帯電話機50等が備えるキーやATM70等が備えるタッチパネル等であり、本認証装置200においては、操作者が、認証装置200との対話したり、バイOMETリックに基づく本人認証を補助するためのIDデータを入力したりする際に用いられる。

【0039】暗号部285は、この認証装置200が通信I/F部230を介して本人認証に関わるデータ(バイOMETリック画像、特徴データ、IDデータ等)を外部装置(認証サーバ30等)に送信する際に、チャレンジレスポンスによる機器間の相互認証を行うとともに時々の秘密鍵を共有化し、その秘密鍵によって送信データを事前に暗号化したり、相互認証の後で外部装置から送信されてきた暗号データに対して秘密鍵を用いて復

号化したりする回路である。

【0040】メモリ部290は、不揮発性のICメモリ等からなる基準データ格納部291及びプログラム格納部292と、揮発性のICメモリ等からなる一時データ格納部293から構成される。基準データ格納部291は、一般的な人の指（左右の手それぞれの親指、人差指）及び目（右目と左目）の輪郭（形状）を示す輪郭基準データ291aを予め格納している。この輪郭基準データ291aは、この認証装置200が本人認証に用いられる被写体の指又は目の位置を認識するために用いられる。

【0041】プログラム格納部292は、(i)鮮明なバイオメトリック画像を取得する等のための制御手順を記述した画像取得プログラム292aと、(ii)取得された特徴データと、認証サーバ30やIDカード110に登録されている特徴データとの照合手順を記述した照合プログラム292bと、(iii)その他の付加的な処理（登録、照合テスト、撮影条件の設定等）手順を記述したユーティリティプログラム292cとを予め格納している。

【0042】一時データ格納部293は、比較対象となる特徴データ293aやIDデータ293b等を一時的に格納する作業領域である。制御部260は、携帯電話機50やATM70等が備えるCPU、RAM及びカレンダー・タイマ回路等からなり、操作者が電子決済をしようとして認証サーバ30等から身元確認をすべき旨の指示を受けたり、操作者からの指示を受けたりしたときに、プログラム格納部292に格納されている対応するプログラム292a～cを実行する。これによって、この認証装置200は、それを備える各通信装置50、60、70及び80の種別等に応じて、以下の機能を発揮する。(1)バイオメトリック画像の取得具体的には、(i)ガイド画像の表示によるバイオメトリック画像の取得（携帯電話機50及びPDA60の場合）と、(ii)追尾制御によるバイオメトリック画像の取得（ATM70やPC80の場合）がある。(2)照合による本人認証具体的には、(i)認証サーバ30への委託による認証（携帯電話機50、PDA60、ATM70及びPC80の場合）と、(ii)IDカード110への委託による認証（ATM70及びPC80の場合）と、(iii)自ら実行することによる認証（ATM70の場合）がある。

(3)ユーティリティ処理具体的には、(i)認証サーバ30又はIDカード110への特徴データの登録と（ATM70及びPC80の場合）、(ii)登録された特徴データをテストするための照合テスト（全ての通信装置50、60、70及び80が対象）と、(iii)撮影条件の設定（全ての通信装置50、60、70及び80が対象）がある。

【0043】次に以上のように構成された電子マネーシステム10の動作について、認証装置200の動作を中

心に説明する。図8は、本認証装置200によるバイオメトリック画像の取得における基本的な動作（通常モード）の手順を示すフローチャートである。なお、本人認証に用いられるバイオメトリック画像の種類（指紋画像のみ、虹彩画像のみ、指紋画像と虹彩画像との組み合わせ等）は、認証サーバ30から認証装置200への通知等によって事前に決定され、制御部260の内部メモリに記憶されている。

【0044】まず、制御部260は、操作者による指示等に基づいて、本人認証に用いられる身体部位（例えば、右手親指）を特定した後に、その身体部位に対応する輪郭基準データ291aを基準データ格納部291から読み出し、その輪郭基準データ291aが示す輪郭を赤い線図（ガイド画像）として画像表示部270に表示する（ステップS300）。

【0045】そして、制御部260は、キャプチャする旨の指示が操作者から発せられるか、又は、1秒等の一定時間が経過するまで、カメラ部240の撮影倍率及び撮影方向の調整による被写体の追尾制御と（ステップS301）、画像処理部250によるバイオメトリック画像の取得及び画像表示部270への表示（ステップS302）とを、繰り返す（ステップS303）。

【0046】具体的には、制御部260は、撮影条件切替部210に対して、身体部位の種類に対応して予め設定されている撮影条件等を送ることによって、カメラ部240のZ駆動部243やθ駆動部242やキャプチャ制御部247を作動させた後に、画像処理部250によるデジタル化によって得られたバイオメトリック画像を取得し、その画像を画像表示部270にカラーで表示出力する。なお、本人認証に用いられる身体部位の種類に応じて、撮影のための適正位置が予め操作者に知らされている。例えば、指であれば、カメラ部240の撮像レンズ244から5cmだけ手前の位置、目であれば、30cmだけ手前の位置等である。

【0047】このような身体部位の動画表示とガイド表示によって、操作者は、画像表示部270に表示されたガイド画像と自分の親指の輪郭とがピッタリと重なり合うように、指や携帯電話機50等を動かして位置調整することができる。そして、適正位置になったと判断したときに、入力部280のボタン等によってキャプチャ指示を発することができる。

【0048】操作者からキャプチャ指示が発せられるか、又は、1秒等の一定時間が経過すると（ステップS303でYes）、制御部260は、上記更新表示（ステップS301～S303）を中断し、直前に取得されたバイオメトリック画像を画像表示部270に静止画として表示出力するとともに（ステップS304）、得られたバイオメトリック画像が適正位置で撮影されたものか否かを判断する（ステップS305～S306）。

【0049】具体的には、制御部260は、画像処理部

250に指示することにより、直前に取得されたバイオメトリック画像から右手親指の輪郭を抽出させ（ステップS305）、その輪郭と輪郭基準データ291aが示す輪郭との一致度（相関値）を算出し、一定の基準値以上であるか否か判断する（ステップS306）。例えば、エッジ検出と2値化等によって、輪郭部分の画素ブロックだけ“1”となる輪郭データを生成し、2つの輪郭データにおける同一位置の画素値どうしの排他的論理和をとり、その結果が“1”となる（画素値が一致する）画素の数を一致度とし、基準値と比較する。

【0050】その結果、一致度が基準値未満である場合には（ステップS306でNo）、制御部260は、それら2つの輪郭について、スケール（撮影倍率）のずれと方向（撮影方向）のずれとを算出し、その結果を撮影条件切替部210に指示することにより、再び、ガイド表示（ステップS301～S303）と輪郭の一致度の判定（ステップS304～S306）とを繰り返す。

【0051】一方、一致度が基準値以上である場合には（ステップS306でYes）、制御部260は、画像処理部250に指示することにより、バイオメトリック画像を切り出した後に指紋の特徴データを抽出させ、その結果（切り出されたバイオメトリック画像と特徴データ）を取得し、一時データ格納部293に格納する（ステップS307）。

【0052】このようにして、認証装置200は、ガイド表示によって、操作者の身体部位を適正な撮影位置に誘導し、身体と接触することなく、予定された大きさと鮮明度のバイオメトリック画像及び特徴データを取得することができる。図9は、高精度モードにおける本認証装置200によるバイオメトリック画像の取得動作の手順を示すフローチャートである。ここで、高精度モードとは、図8に示された取得手順を繰り返す等によってバイオメトリック画像（及び特徴データ）を高精度に取得するオプション的な動作モードであり、操作者から入力部280を介して予め指示される。

【0053】このモードにおいては、認証装置200は、バイオメトリック画像の取得（ステップS313～S316）に先立ち、生体が生きていることを確認する（ステップS310～S312）。これは、死んでいる生体を用いた不正な本人認証を防止する等のためである。具体的には、制御部260は、撮影条件切替部210に指示を出すことにより、（1）ストロボ同期撮影と通常撮影それぞれにおける虹彩画像を取得し、瞳孔の拡大や収縮の有無を検出したり、（2）手や顔全体の撮影を一定時間間隔で繰り返し、得られた画像から抽出した輪郭を比較することにより、生体の動きを検出したりする（ステップS310）。その結果、動きが検出されなかった場合には（ステップS311でNo）、以降の処理を中止し（ステップS312）。

【0054】動きが検出された場合には（ステップS3

11）、予め定められた回数 n だけ、バイオメトリック画像の取得と特徴データの抽出を繰り返す（ステップS313～S316）。具体的には、制御部260は、図8に示される手順を繰り返す。ただし、上記動き検出において、手や顔全体の動きを検出した場合には（ステップS310）、制御部260は、その手又は顔全体の位置を用いて局部（身体部位）の位置を決定し、その身体部位に焦点を合わせるようにカメラ部240のZ駆動部243及び θ 駆動部242を制御する。

10 【0055】このようにして n セットの特徴データが得られると、制御部260は、それら特徴データを平均化することにより、最終的な特徴データとして生成する（ステップS317）。具体的には、指紋の同一特徴点を示す位置座標を平均化したり、アイリスパターンの濃淡値を合計した後に2値化してアイリスコードを生成したりする。

【0056】このようにして、高精度モードによるバイオメトリック画像によれば、時間的な変化画像の平均化により、図8に示された通常モードにおける場合に比べ、撮影に要する時間は少し長くなるものの、生きた生体に対する本人認証が行われ、より高いセキュリティに対応した本人認証が可能となる。図10は、本認証装置200による特徴データの照合における全体的な流れを示すフローチャートである。つまり、本図には、図8や図9に示された手順によって操作者の特徴データ（及びIDデータ）が取得された後における認証装置200の動作手順が示されている。

【0057】まず、制御部260は、リーダライタ部220からの信号に基づいて、IDカード110が装着されているか否か（ステップS320）、及び、装着されている場合には、そのIDカード110のタイプ1～3を検出する（ステップS321）。その結果、タイプ1のIDカード110aが装着されている場合には（ステップS321でタイプ1）、制御部260は、一時データ格納部293に格納されている操作者のIDデータ293bを読み出して暗号部285に暗号化させた後に、通信I/F部230を介して認証サーバ30に送信する（ステップS325）。このときに、送信したIDデータを検索キーとし、その内容に一致する全ての特徴データを返信させる旨の命令も併せて送る。

40 【0058】そして、認証サーバ30から返信されてきた1以上の特徴データを受け取ると、制御部260は、それら受信した特徴データ全てを対象として、既に取得している操作者の特徴データと逐次比較していくことで、一致度を算出する（ステップS326）。その結果、一定のしきい値を超える一致度の特徴データが1つ以上発見された場合には、その操作者を本人と認証し、そうでなければ認証を否定する（ステップS330）。

【0059】一方、タイプ2のIDカード110bが装着されている場合には（ステップS321でタイプ

2)、制御部260は、リーダライタ部220を介してそのIDカード110bから特徴データを読み出し(ステップS324)、その特徴データを認証基準として、上記と同様の照合(ステップS326)と認証(ステップS330)を行う。

【0060】また、タイプ3のIDカード110cが装着されている場合には(ステップS321でタイプ3)、一時データ格納部293に格納されている操作者の特徴データ293aを読み出し、その特徴データと照合させる命令とをリーダライタ部220を介してIDカード110cに送ることで(ステップS322)、IDカード110cに照合を実行させる(ステップS323)。そして、IDカード110cによる照合の結果(一致度)を受け取ると、制御部260は、その照合結果に基づく認証を行う(ステップS330)。

【0061】一方、IDカード110が装着されていない場合には(ステップS320でNO)、制御部260は、その旨を画像表示部270に表示し、それに対して操作者が入力部280を介してIDデータを入力してきたか否か判断する(ステップS327)。その結果、操作者がIDデータを手動で入力してきた場合には(ステップS327でYes)、制御部260は、そのIDデータを、タイプ1のIDカード110aから読み出したIDデータと同様の取り扱いをする(ステップS325~S330)。

【0062】一方、操作者がIDデータの入力を拒否した場合には(ステップS327でNo)、制御部260は、一時データ格納部293に格納されている操作者の特徴データ293aを読み出し、照合させるための命令と共に認証サーバ30に送ることで(ステップS328)、認証サーバ30に対して特徴データだけによる照合を実行させる(ステップS329)。そして、認証サーバ30による照合の結果(一致度)を受け取ると、制御部260は、その照合結果に基づく認証を行う(ステップS330)。

【0063】このようにして、認証装置200は、特徴データに基づく本人認証を行うが、IDデータを利用することができる場合には、そのIDデータを本人認証の補助(検索の高速化)として利用する。また、様々な環境に応じて、認証サーバ30、認証装置200及びIDカード110のいずれかにおいて照合処理が行われ、本人認証に伴う処理負荷の分散が図られる。

【0064】図11は、図10における照合(ステップS323、S326及びS329)及び認証(ステップS330)の詳細な手順、即ち、認証装置200の制御部260、タイプ3のIDカード110cの認証回路及び認証サーバ30により実行される照合及び認証処理の詳細な手順を示すフローチャートである。ここでは、認証装置200の制御部260が指紋と虹彩との組み合わせによる照合と認証を行う場合を説明する。

【0065】制御部260は、カメラ部240等を制御することにより、図8に示された手順に従って、操作者の指紋の特徴データを取得するとともに、予め登録された基準となる指紋の特徴データを認証サーバ30から通信I/F部230を介して取得し、一時データ格納部293に格納する(ステップS340)。そして、それら指紋の特徴データどうしを照合し、その一致度C1を算出する(ステップS341)。例えば、両特徴データそれぞれに含まれる複数の指紋の特徴点のうち、一定範囲内で相対位置が一致する特徴点の個数の割合等を一致度C1として算出する。

【0066】同様にして、制御部260は、操作者の虹彩の特徴データと、登録された基準となる虹彩の特徴データとを取得して一時データ格納部293に格納し(ステップS342)、それら特徴データどうしを照合し、その一致度C2を算出する(ステップS343)。例えば、両特徴データそれぞれに含まれるアイリスコードにおけるハミング距離を求め、それに対応する「確からしさ」の確率を一致度C2として算出する。

【0067】そして、制御部260は、得られた2つの一致度C1及びC2それぞれに対して、予め設定された重み係数k1及びk2を乗じて加算することで総合評価値を出し、その総合評価値が一定のしきい値以上であるか否か判断し(ステップS344)、総合評価値がしきい値以上である場合には(ステップS344でYes)、本人認証を肯定し(ステップS345)、そうでない場合には(ステップS344でNo)、本人認証を否定する(ステップS346)。

【0068】このようにして、認証装置200は、1種類の身体部位だけでなく、複数種類の身体部位による照合を組み合わせることにより、精度の高い本人認証を行うことができる。また、身体部位の種類に応じて、一致度に重み付けをすることで、過去の認証実績に基づいて微妙に判定基準を調整する等の柔軟な本人認証が可能となる。

【0069】なお、登録された基準となる特徴データが複数個ある場合には、特徴データごとに、上記照合と認証を繰り返し、少なくとも1つの特徴データについて本人認証が肯定された場合に、最終的に本人認証を肯定し、全ての特徴データについて本人認証が否定された場合に、最終的に本人認証を否定する。次に、以上のような認証装置200を備える各種通信装置を操作者が使用しているときの様子を説明する。

【0070】図12は、本人認証のために操作者が携帯電話機50に対して右手親指の指紋を提示しているときの様子を示す図である。この携帯電話機50には、LCD53の上方に、バイOMETリック画像を撮影するためのレンズ窓51と発光窓52が設けられている。これらレンズ窓51、発光窓52及びLCD53は、それぞれ、認証装置200のカメラ部240の撮像レンズ24

10

20

30

40

50

4、発光部248、画像表示部270に対応する。

【0071】LCD53には、ガイド画像54と操作者の親指の指紋画像55とが表示されている。操作者は、固定表示されているガイド画像54と自分の指紋画像55の輪郭とがピッタリと一致するように、自分の親指や携帯電話機50を動かして位置調整する。そして、適切な位置で、指と携帯電話機50を一定時間（1秒間等）だけ静止させるか、又は、左手で特定のキーを押すことにより、認証装置200に指紋画像をキャプチャさせる。キャプチャされた場合には、LCD53上の指紋画像は、しばらくの間（基準輪郭と比較されている間）だけ静止表示される。

【0072】図13は、本人認証のために操作者がPDA60に対して右目の虹彩を提示しているときの様子を示す図である。このPDA60には、LCD63の上方に、バイOMETリック画像を撮影するためのレンズ窓61と発光窓62が設けられている。操作者は、図12に示された携帯電話機50の場合と同様にして、LCD63上に固定表示されているガイド画像64と自分の虹彩画像65の輪郭とがピッタリと一致するように、自分の目やPDA60を動かして撮影位置を調整する。そして、適正な撮影位置で、指とPDA60を一定時間（1秒間等）だけ静止させるか、又は、特定のキーを押すことにより、認証装置200に虹彩画像をキャプチャさせることができる。

【0073】図14は、本人認証のために操作者がATM70に対して親指の指紋を提示しているときの様子を示す図である。このATM70には、CRT73の上方に、バイOMETリック画像を撮影するためのレンズ窓71と発光窓72が設けられている。このATM70の認証装置200は、携帯電話機50やPDA60の場合と異なり、カメラ部240による被写体の追尾制御を行うことができる。従って、操作者は、一定範囲の適当な位置に親指を静止させているだけでよい。操作者は、レンズ窓71の動きや、CRT73上のガイド画像74と虹彩画像75の輪郭とがピッタリと一致していくように収束する様子を見ることによって、自動位置調整による撮影が行われていることを感じとることができる。

【0074】図15は、PC80のCRT（認証装置200の画像表示部270）の表示例を示す図である。ここには、認証装置200が有するユーティリティ機能に対応するメニューが表示されている。操作者は、このメニューにおいて、「登録」を選択することで、現時点における自分の指紋や虹彩の特徴データを新たに認証サーバ30又はIDカード110に登録することができる。ただし、既に特徴データが登録されている場合には、その特徴データによる本人認証に成功した後でなければ登録が拒否される。

【0075】また、操作者は、このメニューにおいて、「照合テスト」を選択することで、既に登録されている

特徴データをテストする（認証装置200に現時点での一致度C1及びC2や総合評価値を算出させて表示させる）ことができる。これによって、操作者は、現時点における認証装置200の認証精度を確認したり、既に登録されている特徴データを更新すべきか否かを判断したりすることができる。

【0076】さらに、操作者は、このメニューにおいて、「撮影条件の設定」を選択することで、虹彩に対する撮影条件（ストロボ同期撮影か通常撮影）を選択したり、追尾制御をON/OFFしたり、バイOMETリック画像の取得モード（通常モードか高精度モード）を設定したり、繰り返し撮影における繰り返し回数nを指定したり、本人認証に使用される身体部位やその組み合わせを指定したりすることができる。

【0077】なお、これらユーティリティメニューにおける処理は、認証装置200の制御部260が、入力部280及び画像表示部270を介して操作者と対話しながら決定していく。そして、決定されたパラメータは、メモリ部290や制御部260の内部の不揮発メモリ等に格納され、画像取得プログラム292a等の実行時に用いられる。

【0078】以上、本発明に係る認証装置及び電子マネーシステムについて、実施の形態に基づいて説明したが、本発明はこの実施の形態に限られないことは勿論である。例えば、本発明の本人認証は、通信ネットワーク20に接続され、認証サーバ30と通信しながら本人認証を実行する電子マネーシステム10に用いられたが、他の様々な用途に適用することができる。

【0079】図16は、本発明に係る本人認証をキーレスの用途に応用した例を示す図である。図16(a)は、キーレスマンションの入退室管理への適用例を示すイメージ図である。マンションの共同玄関400に設置された認証装置402で取得されたバイOMETリック画像と特徴データは、各戸410に設置された認証サーバ機能付きインターフォン411に配信される。そして、この認証サーバ機能付きインターフォン411によって本人認証が成功した場合に、それと連動した玄関扉412のロックが解除される。このようなビル管理システムによって、居住者は、認証サーバ機能付きインターフォン411に予めバイOMETリック情報を登録しておくだけで、鍵を持ち歩かなくとも、また、パスワードを忘れてしまっても、ロックアウトされる心配がない。従って、ビルディングの各戸への入退室におけるセキュリティと利便性が増す。

【0080】図16(b)は、キーレス自動車への適用例を示すイメージ図である。この自動車420は、キーのロック機構と連動した認証装置421を搭載している。認証装置421には、この自動車420の持主のバイOMETリック情報が予め登録されている。持主は、この認証装置421に対して自分の指紋や虹彩を提示し、

本人認証に成功してからでないと、キーを差し込んで回転させることができない。つまり、本人認証に成功することによって、初めてエンジンを始動させることができる。これによって、車の盗難が防止される。

【0081】図17は、本発明に係る本人認証を自動販売機に適用した例を示すイメージ図である。この自動販売機430は、上記実施の形態における認証装置200と同等機能の認証装置431と、その認証装置431により本人認証が成功した場合に、指定された商品を取り出し口に移動させる制御回路等を備える。予め認証サーバにバイOMETリック情報が登録された会員（例えば、この自動販売機430が設置されているビル内で働く従業員等）は、専用カードを使用することなく、又は、専用カードの使用とともに、指紋や虹彩を認証装置431に提示することにより、現金を持ち合わせることなく、電子決済によるその場での商品購入をすることができる。

【0082】さらに、本発明に係る本人認証をPOS（Point Of Sales）システムに適用することもできる。例えば、スーパーマーケットにおけるレジスター等のPOS端末装置に本実施の形態の認証装置200を装備させ、POSシステムにおけるサーバコンピュータに本実施の形態の認証サーバ30を装備させればよい。これによって、本実施の形態におけるATM70等と同様の入出金処理等が可能となる。つまり、ショッピング等においてパスワードやクレジットカード等が不要になるだけでなく、よりセキュリティの高い本人認証による決済が可能となる。

【0083】また、本実施の形態では、バイOMETリック画像を取得する認証装置200と、特徴データのデータベースを備える認証サーバ30とは別個独立した装置であったが、これらを一体化させてもよい。これによって、バイOMETリック画像の取得と本人認証とを実行するスタンドアローンの本人認証装置が実現される。また、本実施の形態の認証装置200においては、画像処理部250がデジタルフィルタ等を用いて特徴データを生成したが、これに代えて、制御部260がソフト的に（CPUに特徴抽出プログラムを実行させることによって）特徴データを生成する構成としてもよい。

【0084】また、本実施の形態では、本人認証に用いられるバイOMETリックの対象は、指紋と虹彩であったが、掌形（手の大きさ、長さ、厚さ、比率等）、顔形（顔の輪郭、目や鼻の形及び配置等）、静脈（手の甲の静脈パターン）、耳介（耳輪や耳甲介腔の大きさ、耳甲介腔幅、耳甲介腔長、形態的耳長等）を加えてもよい。そして、これら身体部位の中から本人認証に用いるものをユーザが選択してもよい。例えば、認証サーバ30に登録されたデータベースに基づいて、本人認証に用いることが可能な複数の身体部位をPDA60のファンクションキーf1～f10それぞれに割り当てて表示してお

き、いずれかのファンクションキーがユーザに押された場合に、そのキーに対応する身体部位を用いた本人認証を実施することとしてもよい。これによって、ユーザの都合に応じた本人認証や、最もセキュリティが高いとユーザが信じる身体部位による本人認証が実現される。

【0085】また、本実施の形態では、生体が活着していることを確認するために、瞳孔の動きが検出されたが、これに代えて、黒目の動き、まばたきの有無を検出することとしてもよい。また、本電子マネーシステム10における照合においては、特徴データが比較され、バイOMETリック画像そのものは直接的には用いられなかったが、特徴データに代えて、又は、特徴データに加えて、バイOMETリック画像そのものを照合の対象としてもよい。これによって、原画像に基づく本人認証が可能となり、認証サーバ30やIDカード110における最新の照合アルゴリズムに基づく精度の高い本人認証が実現される。

【0086】

【発明の効果】以上の説明から明らかなように、本発明に係る本人認証装置は、バイOMETリックに基づいて本人認証を行う装置であって、非接触で身体部位を撮影することによりバイOMETリック画像を取得する撮影手段と、取得されたバイOMETリック画像を表示するバイOMETリック画像表示手段と、適正な撮影位置で前記部位が撮影された場合の部位の外形を示すガイド画像を前記バイOMETリック画像に重ねて表示するガイド表示手段と、前記バイOMETリック画像に基づいて、前記部位が適正な撮影位置で撮影されたか否かを判断する判断手段と、適正な撮影位置で撮影されたか判断された場合に、前記バイOMETリック画像から前記部位の形態的な特徴を示すバイOMETリック情報を抽出し、予め登録されたバイOMETリック情報と照合することにより、本人認証を行う認証手段とを備えることを特徴とする。

【0087】これによって、非接触でバイOMETリック画像が採取され、本人認証が行われるので、接触センシングに起因する従来の不具合は解消される。そして、画像表示手段にはバイOMETリック画像だけでなく、適正な撮影位置を示すガイド画像も同時に表示されるので、操作者は、それら画像が重なるように身体部位を移動させることにより、ビントの合った鮮明なバイOMETリック画像に基づく本人認証を行うことができる。

【0088】ここで、前記本人認証装置は、さらに、適正な撮影位置で前記部位が撮影されるように前記撮影手段による撮影の方向と倍率とを制御する撮影制御手段を備えてもよい。これによって、操作者は、本人認証に用いる身体部位を適当な空間位置で静止させているだけで、本人認証装置の追尾制御による自動撮影が行われる。

【0089】また、前記本人認証装置は、さらに、前記部位又は前記部位を含むより大きな部位を繰り返して撮

影するように前記撮影手段を制御し、得られた複数の画像に基づいて、身体の動きを検出する動き検出手段を備え、前記認証手段は、前記動き検出手段によって身体の動きが検出され、かつ、前記部位が適正な撮影位置で撮影されたと判断された場合に、本人認証を行ってもよい。これによって、動きが確認された身体部位による本人認証、即ち、生きた生体による本人認証が行われ、死体を用いた不正な本人認証が防止される。

【0090】また、前記部位は、虹彩であり、前記動き検出手段は、前記虹彩に光を照射するとともに、その照射に同期して虹彩を撮影するように前記撮影手段を制御してもよい。これによって、瞳孔が萎んだ状態での虹彩、即ち、より面積の大きい状態での虹彩による本人認証が行われ、認証精度が向上される。また、光に対する瞳孔の反応（拡大・収縮）の有無を検出することで、生体が生きているか否かを確認することも可能となる。また、前記本人認証装置は、さらに、繰り返して前記部位を撮影するように前記撮影手段を制御する繰り返し制御手段を備え、前記認証手段は、繰り返し撮影によって得られた複数のバイオメトリック画像に基づいて前記バイオメトリック情報を抽出し、本人認証を行ってもよい。これによって、身体部位の動きを検出することが可能となるので、生体が生きていることを確認した後に本人認証を行うことができる。

【0091】また、前記本人認証装置は、さらに、身体部の複数の部位について、前記バイオメトリック画像を取得し、取得されたバイオメトリック画像を表示し、前記ガイド画像を表示し、前記部位が適正な撮影位置で撮影されたか否かを判断するように前記撮影手段と、前記バイオメトリック画像表示手段と、前記ガイド表示手段と、判断手段とを制御する複数の部位制御手段を備え、前記認証手段は、取得された複数の部位のバイオメトリック画像から複数の部位についてのバイオメトリック情報を抽出し、それらバイオメトリック情報の組み合わせと予め登録された対応するバイオメトリック情報の組み合わせとを照合することにより、本人認証を行ってもよい。例えば、指紋と虹彩の組み合わせとしてもよい。

【0092】これによって、1種類の身体部位だけによる本人認証よりも高い精度で認証が行われる。また、同一の撮影手段により、複数の身体部位に基づく本人認証が行われるので、2以上の種類のセンサを組み合わせる本人認証する場合に比べ、低コストとなる。また、前記認証手段は、前記複数の部位ごとの照合結果を示す一致度それぞれに異なる重みづけをした後に加算して得られる総合評価値が一定のしきい値を超えるか否かによって、前記本人認証を行ってもよい。これによって、身体部位の種類に応じた重み付けができるので、きめの細かい高精度な本人認証が実現される。

【0093】また、前記複数の部位は、異なる指の指紋としたり、両目の虹彩としてもよい。これによって、ほ

ぼ同じ撮影位置で複数の身体部位による本人認証が可能となり、撮影条件の変更が少なく済む。また、前記本人認証装置は、さらに、前記撮影に伴って、本人の識別に役立つ情報であるIDデータを取得するIDデータ取得手段を備え、前記認証装置は、前記バイオメトリック情報及び前記IDデータの組み合わせと予め登録されたバイオメトリック情報及びIDデータの組み合わせとを照合することにより、本人認証を行ってもよい。これによって、本人認証の精度が向上される。

【0094】また、前記認証手段は、予め登録された複数のバイオメトリック情報の中から、IDデータが一致するものを特定し、特定したバイオメトリック情報と抽出された前記バイオメトリック情報との同一性によって、本人認証を行ってもよい。これによって、バイオメトリック情報による照合に先立って、IDデータを用いた検索対象の絞り込みが行われるので、本人認証に要する処理時間が削減される。

【0095】また、前記認証装置は、さらに、予め登録された前記バイオメトリック情報を記憶する記憶手段と、前記記憶手段に記憶されたバイオメトリック情報を前記認証手段により抽出されたバイオメトリック情報で置き換える登録情報更新手段を備えてもよい。これによって、更新可能なデータベース（登録されたバイオメトリック情報群）を備えるスタンドアロンタイプの本人認証装置が実現される。

【0096】また、前記更新手段は、予め定められた一定期間を超えてバイオメトリック情報が更新されていない場合に、前記バイオメトリック情報を置き換えてもよい。これによって、登録データベースは最新のものに維持されるので、高い精度による本人認証が継続される。以上のように、本発明は、ユーザに心理的な不快感や嫌悪感を与えることのない非接触センシングによる低コストで、かつ、複数のバイオメトリック画像に基づく高い精度の本人認証を行うことができ、その実用的価値は極めて高い。

【図面の簡単な説明】

【図1】本発明に係る電子マネーシステムの全体構成を示す図である。

【図2】同システムにおける認証サーバに備えられているデータベースの内容を示す図である。

【図3】(a)は、IDデータだけが記録された最も簡単なタイプ1のIDカード、(b)は、さらに特徴データが記録されたタイプ2のIDカード、(c)は、さらに認証回路を備える最も高機能なタイプ3のIDカードの概観図である。

【図4】同システムのATM等が備える認証装置の構成を示すブロック図である。

【図5】同認証装置のカメラ部の詳細な構成を示すブロック図である。

【図6】同認証装置の画像処理部が生成する指紋の特徴

データを説明するための図である。

【図7】同認証装置の画像処理部が生成する虹彩の特徴データを説明するための図である。

【図8】通常モードにより認証装置がバイオメトリック画像を取得する場合の動作手順を示すフローチャートである。

【図9】高精度モードにより認証装置がバイオメトリック画像を取得する場合の動作手順を示すフローチャートである。

【図10】同認証装置による特徴データの照合における全体的の流れを示すフローチャートである。

【図11】図10における照合及び認証処理の詳細な手順を示すフローチャートである。

【図12】同認証装置を備える携帯電話機を用いて操作者が本人認証をしている様子を示す図である。

【図13】同認証装置を備えるPDAを用いて操作者が本人認証をしている様子を示す図である。

【図14】同認証装置を備えるATMを用いて操作者が本人認証をしている様子を示す図である。

【図15】同認証装置が有するユーティリティ機能に対応するメニューの表示例である。

【図16】(a)は、同認証装置をキーレスマンションの入退室管理に適用した例を示すイメージ図であり、

(b)は、キーレス自動車に適用した例を示すイメージ図である。

【図17】同認証装置を自動販売機に適用した例を示すイメージ図である。

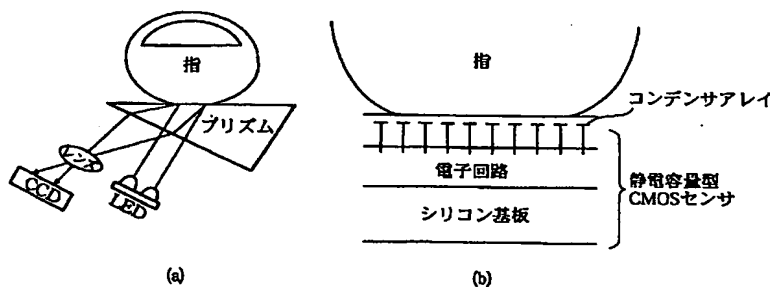
【図18】従来の認証装置が備えるバイオメトリックセンサの例を示し、(a)は、光学式指紋スキャナと呼ばれる方式、(b)は、静電容量型指紋センサチップによる方式を示す図である。

【符号の説明】

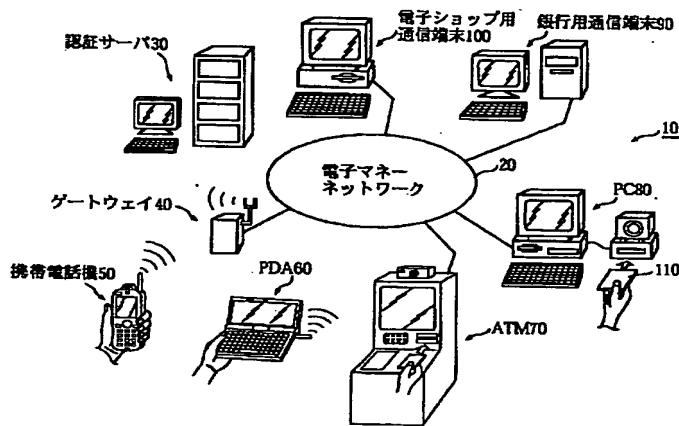
- 10 電子マネーシステム
- 20 通信ネットワーク
- 30 認証サーバ
- 40 ゲートウェイ
- 50 携帯電話機

- * 60 PDA
- 70 ATM
- 80 PC
- 90 銀行用通信端末
- 100 電子ショップ用通信端末
- 110 IDカード
- 200 認証装置
- 210 撮影条件切替部
- 220 リーダライタ部
- 230 通信I/F部
- 240 カメラ部
- 241 可動部
- 242 駆動部
- 243 Z駆動部
- 244 撮像レンズ
- 245 イメージセンサ部
- 246 AF制御部
- 247 キャブチャ制御部
- 248 発光部
- 250 画像処理部
- 260 制御部
- 270 画像表示部
- 280 入力部
- 285 暗号部
- 290 メモリ部
- 291 基準データ格納部
- 292 プログラム格納部
- 293 一時データ格納部
- 400 共同玄関
- 402 認証装置
- 410 各室内
- 411 認証サーバ機能付きインターフォン
- 412 玄関扉
- 420 自動車
- 421 認証装置
- 430 自動販売機
- * 431 認証装置




【図18】



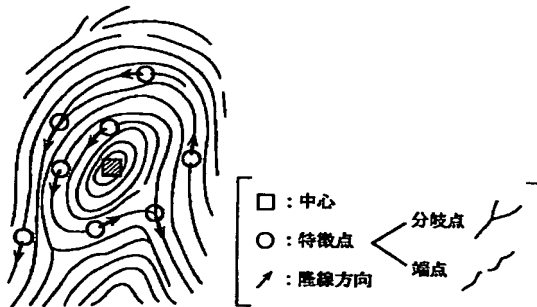
【図1】



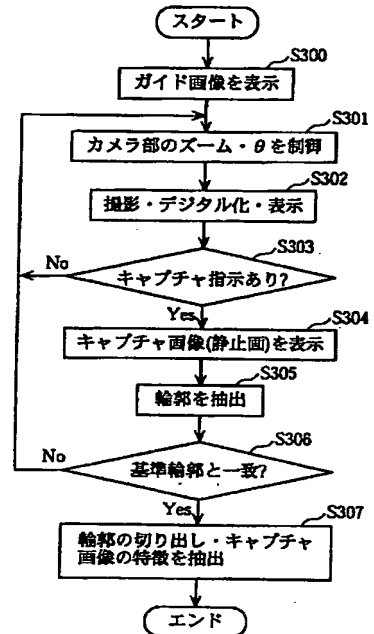
【図2】

PIC(個人識別コード)	IDデータ	バイオメトリック画像	特徴データ	その他
5678abcd124	名前		bio_ID=右手親指 中心・分岐点・端点の位置 屈線方向	登録年月日
	生年月日		bio_ID=左目虹彩 アイリスコード	登録年月日
	住所		bio_ID=右目虹彩 アイリスコード	登録年月日
	電話番号			
	パスワード			

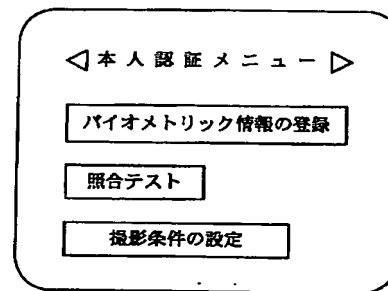
【図6】



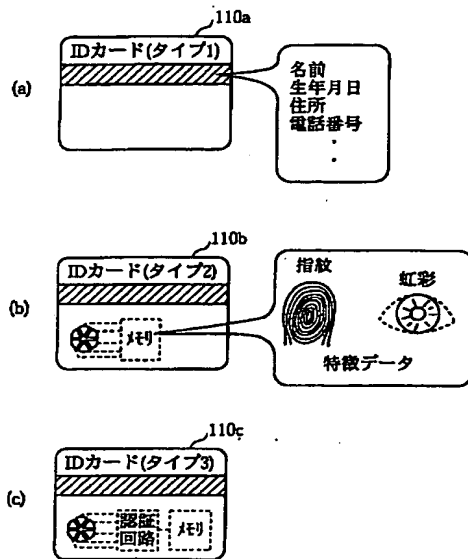
【図8】



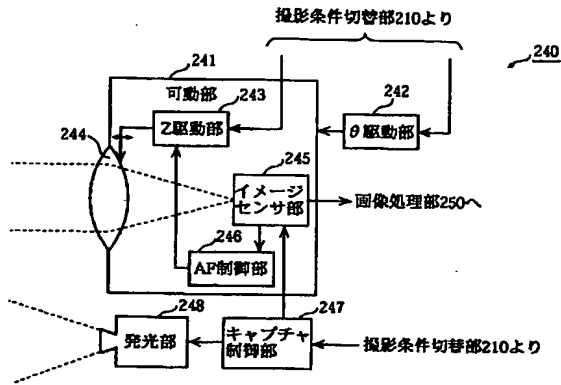
【図15】



【図3】

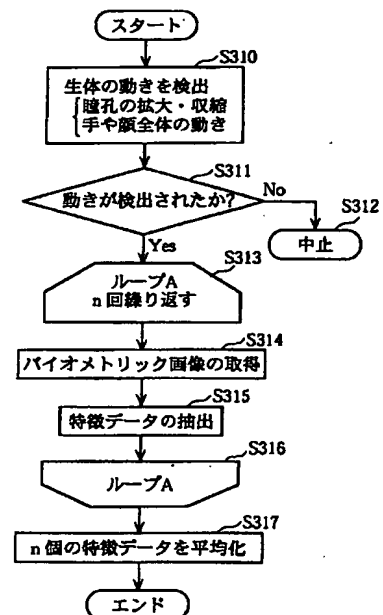
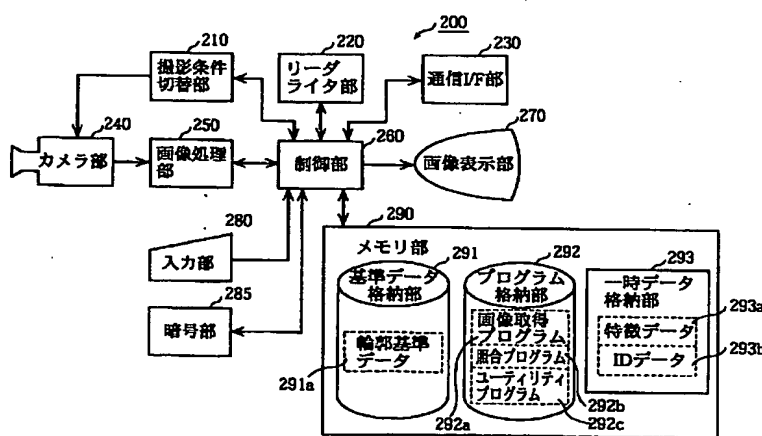


【図5】

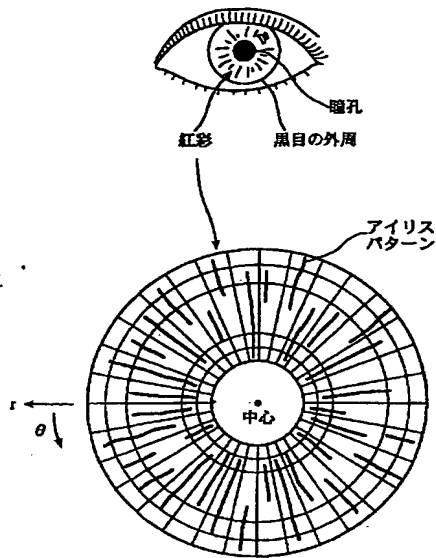


【図9】

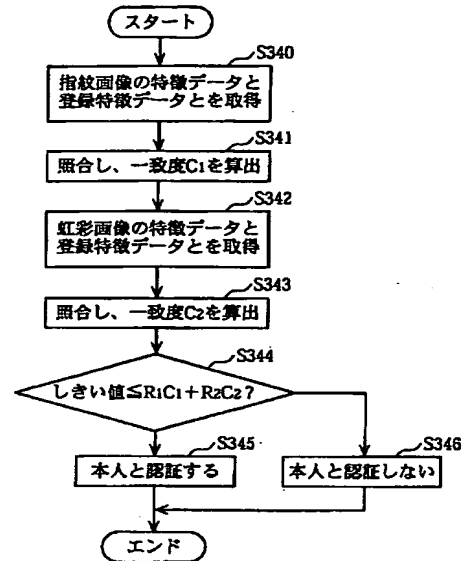
【図4】



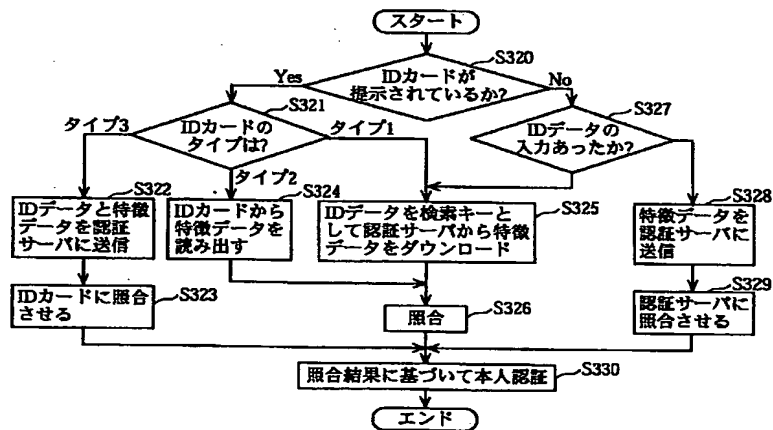
【図7】



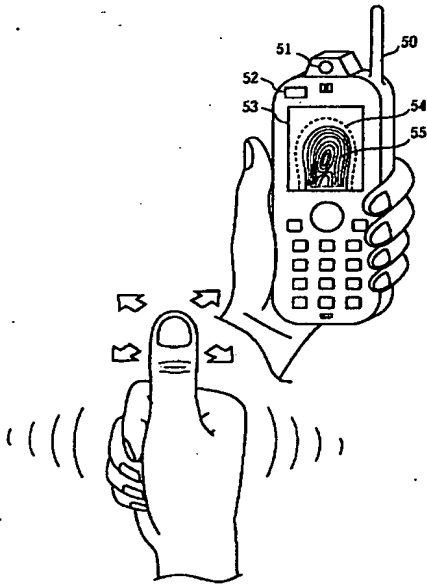
【図11】



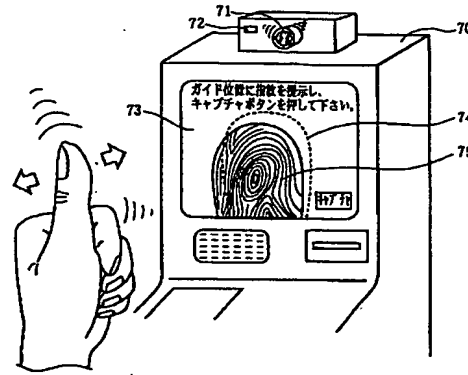
【図10】



【図12】

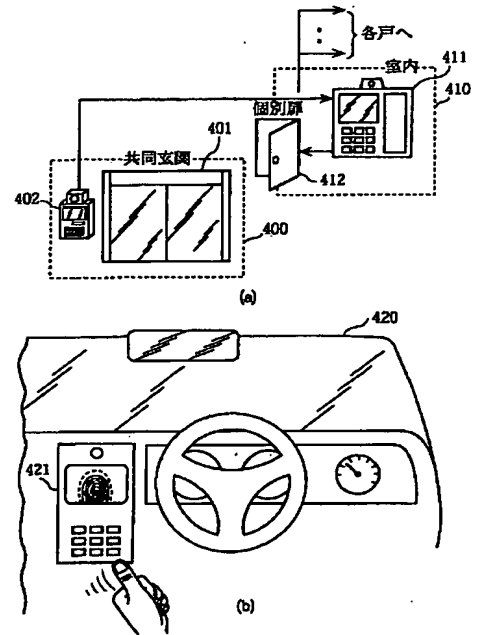
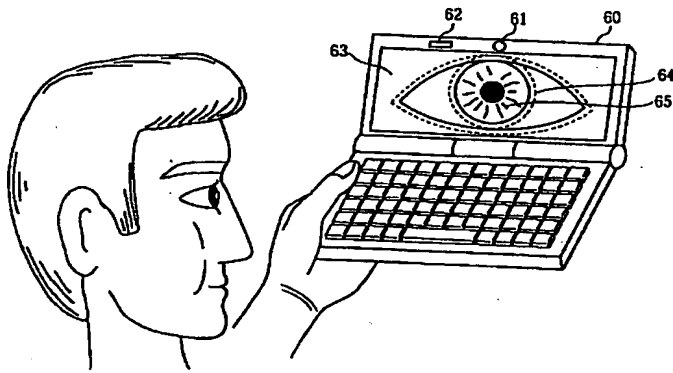


【図14】

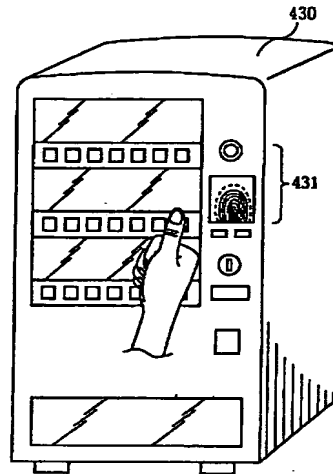


【図16】

【図13】



【図17】



フロントページの続き

(51)Int.Cl. ⁷	識別記号	F I	ターム (参考)
G 0 6 K 19/10		G 0 6 T 1/00	4 0 0 H 5 B 0 8 5
G 0 6 T 1/00	4 0 0	A 6 1 B 5/10	3 2 0 Z 5 J 1 0 4
		G 0 6 K 19/00	S
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 D
			6 7 3 A

F ターム (参考) 4C038 VA07 VB04 VB13 VC01 VC05
 5B035 BB02 BB03 BB09 BC01 CA11
 5B043 AA01 AA04 AA09 BA02 BA04
 CA09 EA06 EA15 FA02 FA03
 FA04 GA02 GA13 HA11
 5B047 AA23 AA25
 5B058 CA01 KA38 YA02 YA11 YA13
 5B085 AE23 AE25
 5J104 AA07 KA01 KA16 KA17 NA34
 NA35 NA36 NA38 PA02 PA10
 PA12 PA16